The Naval Surface Warfare Center Dahlgren Division

The U.S. Marine Corps, Army, Coast Guard and National Guard select NSWCDD as their primary CWID 2005 site

By John J. Joyce

The Naval Surface Warfare Center Dahlgren Division (NSWCDD) is uniquely positioned to help navigate the Navy's road to transformation. Its broad spectrum of resources, including its workforce and infrastructure have made it a premier naval scientific and engineering institution dedicated to solving a diverse set of complex technical problems confronting the warfighter.

NSWCDD fills a major role in the annual Coalition Warrior Interoperability Demonstration (CWID). The demonstration tests and evaluates technologies and capabilities focused on selected core objectives defined by combatant commanders.

The NSWC Dahlgren CWID lab site team, back row (l-r) Robert Hill, Dennis Warne (site manager), Mike Cajohn (Marine Corps liaison), Hank St. Laurent (site lead engineer) and Benjamin McCormick. Front row (l-r) Mike Remington, Ralph Thompson (deputy site manager), Sean Cunningham, Steve Horowitz and Timothy Williams.

CWID focused on homeland security (HLS), homeland defense (HLD) and coalition interoperability. U.S. Joint Forces Command (USJFCOM) provided planning and execution oversight for the worldwide event that was conducted in a simulated operational environment June 13–23, 2005.

"Location and cost effectiveness have been crucial to the success and growth of CWID at NSWC Dahlgren. It is good economics for us to host more than one service, the Army, Marine Corps, Coast Guard, National Guard and Navy, because the services share a lot of the same systems: CONOPS (concept of operations), infrastructure and the networks required for CWID," McGettigan said.

"This is the seventh year that NSWC Dahlgren has been a JWID/CWID site. We began in 1999 with only the Marine Corps. Since then, we have hosted additional services and continue to build successful working relationships with a multitude of commands and organizations," said Capt. Joseph McGettigan, commander of NSWCDD.

CWID Participants

The demonstration involved 26 countries, including Australia, Canada, New Zealand, United Kingdom and many NATO nations. Participants interacted in a scripted scenario over a global network at 30 sites around the world. For the first time in CWID 2005, decision makers from government agencies, national and international law enforcement organizations and first responders worked alongside our traditional military allies.

"I got the impression that everyone here was trying to help the guys at the front — to save the lives of warfighters, said New Zealand Army Lt. Col. Tony Hill.

More than 40 technology trials were assessed for interagency information sharing and coalition interoperability under the leadership of the host combatant commander, U.S. Northern Command (USNORTHCOM), Peterson Air Force Base, Colo., and the executive agent, the Defense Information Systems Agency (DISA), Arlington, Va. USNORTHCOM works with key interagency partners to identify new ways to improve cooperation, coordination and information sharing.

Secret Sharing

There were two major network enclaves for CWID: (1) The warfighter enclave – the secret network of coalition and guest nations, and (2) The HLS/HLD enclave – the network for homeland security. The Coalition Secret Network or "purple" enclave stood up for the first time to release secret classified information to the 26 coalition members. Nations were grouped into communities of interest separated by flexible, cost-effective virtual private networks and firewall managers that permitted controlled, protected communications, instead of security enclaves that required the use of Type-1 encryption devices and costly approved guards.

The purple network was a huge success, according to DISA CWID Joint Management Office Director, Air Force Lt. Col. Buddy Dees. "We had a stronger coalition exchange of information since everyone agreed that information put on the purple enclave was releasable to all participants of a coalition force," Dees said. "We were able to show that the technology is trustworthy."

A "black" domain for unclassified sharing was also used throughout the worldwide demonstration. Warfighters from Norway to New Zealand assessed the effectiveness of 52 interoperability trials in a realistic environment for possible operational use in the Global Information Grid within 18 months of the execution period.

CWID organizers required each trial to address at least one of the demonstration's core objectives: mission assurance; situational

awareness; multilevel/multidomain protection; collaborative information environment; intelligence, surveillance and reconnaissance dissemination; wireless security; language translation; and integrated logistics. What's more, the CWID scenario merged aspects of HLS and HLD with coalition operations so the demonstration could be used as a proving ground for emerging technologies through the entire spectrum of first responders.

Meeting the goal to move promising technologies through the CWID process from the demonstration to the field within six to 18 months has been a persistent challenge in the wake of past demonstrations and this CWID is no different.

"According to the Naval Sea Systems-NSWC Enterprise Charter, we want to accelerate technology into affordable capability for the warfighter. At Dahlgren, we apply research and development, science and technology, and test and evaluation to deliver technological solutions to today's warfighters and reshape the future Navy," McGettigan said.

Fielding promising CWID technologies results in a combined effort that includes DISA, the Joint Staff, Joint Systems Integration Command and USJFCOM's Command, Control, Communications, and Computer (C4) Systems Directorate (J6) and Joint Requirements and Integration Directorate (J8).

Defining Roles and Responsibilities

According to Dennis Warne, CWID site manager for the NSWCDD lab, there were some challenges in the HLD/HLS scenarios in dealing with county and state first responders, who do not have DoD clearances or equivalent security clearances.

"What is considered sensitive, classified or unclassified in a multifunctional environment? Another challenge in CWID is how do you define warfighters? This is not a real term when you are dealing with fire, police, rescue or emergency personnel. They are not warfighters, at least not in the traditional sense," Warne said. "A lot of these questions still need to be determined by policy, laws, concept of operations, and tactics, techniques and procedures."

Warfighter Collaboration

At Dahlgren, active duty and Reserve warfighters collaborated with industry representatives to discover innovative ways to apply the solutions they were testing on the Combined Forces Battle Laboratories Network, which merged HLD and coalition task force (CTF) operations into one integrated scenario.

The scenario consisted of two parts: one for HLS and HLD and the other for the CTF. In the HLS/HLD scenario, USNORTHCOM with local, state and federal agencies responded to terrorist attacks within the United States. These fictitious attacks were tied to conventional U.S.-led CTF operations on another continent.

For the CTF portion of the demonstration, CWID provided a framework to facilitate interoperability trials through a full range of military operations conducted by U.S. and coalition forces. CTF operations were set in a hypothetical context that involved imaginary countries. Contrasting the theoretical backdrop was

L-R: Marine Corps Lt. Gen. Robert Shea, Joint Staff Director, Command, Control, Communications and Computer (C4) Systems (J6); Army Maj. Gen. Dennis Moran, Joint Staff Vice Director for C4; and Army Maj. Corey Brumsey are briefed by Information Systems Technician 3rd Class Ricky Payne at NSWCDD during CWID trials.

a very real focus on valid capabilities that can be delivered to the warfighter quickly.

"This CWID approach fits in with the way that we harness the intellectual capital of our workforce to put technology into the hands of the warfighter to solve their problems today. CWID also fits in with the work that we do designing the Navy *Next* and the Navy after that. Many joint efforts in both the RDT&E (research, development, test and evaluation) realm and operational tasks are performed at NSWC Dahlgren. Our customers reach beyond the Navy to the Office of the Secretary of Defense, the other services and other government agencies," McGettigan said.

DISA managed the event's day-to-day operations and engineered the demonstration network. The agency set up a demonstration architecture that enabled controlled and protected communications as prescribed by operational requirements and national security policies.

According to Warne, there were no disappointments with any of the technologies tested.

"We don't look at them that way. They either executed to their requirements or they didn't. We do not want to drop a trial just because it did not come up number one or number two. Some are just more mature than others, and some need to be reassessed," Warne said.

The next CWID is planned for May 30–June 23, 2006. For more information, go to the CWID home page at http://www.cwid.js.mil/.

For more information about NSWCDD go to http://www.nswc.navy.mil.

John Joyce is part of the NSWCDD Corporate Communications Office and a Navy Reservist serving with the USJFCOM Joint Public Affairs Support Element.   CHIPS